(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 21 686 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
H 04 L 12/22

(21) Aktenzeichen: 100 21 686.2
(22) Anmeldetag: 5. 5. 2000
(43) Offenlegungstag: 8. 11. 2001

DE 100 21 686 A 1

(71) Anmelder:
Deutsche Thomson-Brandt GmbH, 78048 Villingen-Schwenningen, DE

(72) Erfinder:
Platte, Hans-Joachim, Dr., 30966 Hemmingen, DE;
Fleischer, Wolfgang, 30171 Hannover, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:
US 56 75 711

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Reduktion der Verbreitung von Computerviren in einem elektronischen Mail-Netzwerk

(57) Die Erfindung betrifft ein Verfahren zur Reduktion der Verbreitung von Computerviren in einem elektronischen Mail-Netzwerk.
In einem Mailserver mit einer Vielzahl angeschlossener Mailteilnehmer-Computer ist ein Verfahren installiert, mit dem an die Teilnehmer nacheinander eingehende oder von den Teilnehmern nacheinander ausgehende Mails auf bestimmte Gemeinsamkeiten geprüft werden und in Abhängigkeit von festgestellten Gemeinsamkeiten entweder die Mails bestimmungsgemäß automatisch weitergeleitet oder bis zum Eintreten eines anderen Kriteriums zurückgehalten werden.

DE 100 21 686 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Reduktion der Verbreitung von Computerviren in einem elektronischen Mail-Netzwerk.

Stand der Technik

[0002] In der heutigen Zeit elektronischer Mails und weltweiter Vernetzung von Computern bilden viele Formen von sogenannten Computerviren eine große Gefahr für Firmen, die ihre in Netzwerken verbundenen Computer auch mit der elektronischen Außenwelt verbunden betreiben. An den Verbindungsstellen zur elektronischen Außenwelt, wie zum Beispiel dem Internet, werden spezielle Computer als sogenannten Firewalls betrieben, die u. a. versuchen, mit elektronischen Viren behaftete Mails von außen herauszufiltern bevor diese die firmeneigenen Computer erreichen können. Die Erkennung eines Virus erfolgt durch spezielle Software, die jeweils vom Hersteller auf dem Stand der neuesten Viren-Pattern gehalten werden muß.

[0003] Zwischen Auftreten eines neuen Virus und der Erzeugung und Verbreitung eines neuen Viren-Patterns vergeht jedoch eine gewisse Zeit, in der der Virus erhebliche Schäden anrichten kann. Die Methode des Viren-Erkennens im Firewall-Computer ist somit grundsätzlich anfällig. Denn zur Herstellung eines Viren-Patterns muß zunächst ein Virus bekannt werden, was üblicherweise schon mit einem Schadensfall verbunden ist. Wird ein Virus vom Urheber geschickt und breit gleichzeitig in Firmennetzwerke eingeschleust, so wird die Schadensbegrenzung ein Wettlauf mit der Zeit zwischen der Virenausbreitung und dem Erstellen und Installieren von Erkennungsprogrammen. Durch besondere Strukturen kann der Virus innerhalb von wenigen Stunden, die die Erstellung eines Erkennungsmusters benötigt, erhebliche Schäden anrichten, indem er die befallenen Computer zum Beispiel zur schneeballartigen Aussendung von Kopien seiner selbst an alle in diesem Computer gespeicherten Mail-Adressen veranlaßt.

Erfindung

[0004] Ziel dieser Erfindung ist die Begrenzung bzw. Unterbrechung der schneeballartigen Weiterverteilungskette des Virus.

[0005] Die Erfindung wird durch die im Anspruch 1 angegebenen Merkmale gelöst.

[0006] Vorteilhafte Weiterbildungen sind in den Unteransprüchen wiedergegeben.

[0007] Erfindungsgemäß wird in einem Mailserver mit einer Vielzahl angeschlossener Mailteilnehmer-Computer ein Verfahren installiert, mit dem an die Teilnehmer nacheinander eingehende oder von den Teilnehmern nacheinander ausgehende Mails auf bestimmte Gemeinsamkeiten geprüft werden und in Abhängigkeit von festgestellten Gemeinsamkeiten entweder die Mails bestimmungsgemäß automatisch weitergeleitet oder bis zum Eintreten eines anderen Kriteriums zurückgehalten werden.

[0008] Als Kriterium der festgestellten Gemeinsamkeit kann das Auftreten der selben Betreffzeile in einer Mehrzahl von Mails sein, das Auftreten des selben Inhaltstextes, eines gleichen Attachments und/oder die selbe oder zeitnahe Absende- oder Empfangszeit gewählt werden.

[0009] In dem Fall, dass eine elektronische Mail aufgrund einer oder mehrerer dieser Kriterien automatisch zurückgehalten wird, kann eine Mail-Rückfrage durch den Mailserver dem absendenden Mailteilnehmer zugeleitet werden, ob dieser alle mit erheblichen Gemeinsamkeiten versehene Mails wirklich verschicken will und dieser absendende Mailteilnehmer darauf mit einer expliziten Bestätigung antwortet.

[0010] Als eine "explizite Bestätigung" des absendenden Mailteilnehmers kann vorzugsweise die Eingabe einer Kennung oder eines Passwortes dienen.

[0011] Alternativ oder als ein weiteres "anderes Kriterium" kann eine Mail-Rückfrage bei dem Administrator des betreffenden Netzwerkes sein, ob dieser alle mit erheblichen Gemeinsamkeiten versehenen Mails wirklich verschickt sehen will und dieser Administrator darauf mit einer expliziten Bestätigung antwortet.

[0012] Vorzugsweise können solche gekennzeichneten elektronischen Mails auch nach Ablauf einer verzögernden Zeit weitergeleitet werden. Die Zeitverzögerung sollte dann vorteilhaft so groß sein, daß auf eine Virenwarnung von außerhalb reagiert werden kann oder in einen vorgegebenen Zeitrahmen fallen, zum Beispiel in die normale Arbeitszeit des Administrators.

Patentansprüche

1. Verfahren zur Reduktion der Verbreitung von Computerviren in einem elektronischen Mail-Netzwerk mit einem Mailserver und einer daran angeschlossenen Vielzahl von Mailteilnehmer-Computern durch an die Teilnehmer nacheinander eingehende oder von den Teilnehmern nacheinander ausgehende Mails, **dadurch gekennzeichnet**, dass die an die Teilnehmer nacheinander eingehenden oder von den Teilnehmern nacheinander ausgehenden Mails auf bestimmte Gemeinsamkeiten geprüft werden und in Abhängigkeit von festgestellten Gemeinsamkeiten entweder die elektronischen Mails bestimmungsgemäß automatisch weitergeleitet werden oder bis zum Eintreten eines anderen Kriteriums zurückgehalten werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als Kriterium der festgestellten Gemeinsamkeit das Auftreten der selben Betreff-Zeile in einer Mehrzahl von Mails, das Auftreten des selben Inhaltstextes, eines gleichen Attachments und/oder die selbe oder zeitnahe Absende- oder Empfangszeit verwendet wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass in dem Fall, dass eine elektronische Mail aufgrund einer oder mehrerer dieser Kriterien automatisch zurückgehalten wird, eine Mail-Rückfrage durch den Mailserver dem absendenden Mailteilnehmer zugeleitet wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass diese mit erheblichen Gemeinsamkeiten versehenen Mails durch den Mailserver verschickt werden, wenn der absendende Mailteilnehmer die Mail-Rückfrage durch den Mailserver mit einer expliziten Bestätigung bestätigt.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass als eine "explizite Bestätigung" des absendenden Mailteilnehmers vorzugsweise die Eingabe einer Kennung oder eines Passwortes dient.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als ein weiteres anderes Kriterium eine Mail-Rückfrage bei dem Administrator des betreffenden Netzwerkes durchgeführt wird, ob dieser alle mit erheblichen Gemeinsamkeiten versehenen Mails wirklich verschickt sehen will und dieser Administrator darauf mit einer expliziten Bestätigung antwortet.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass solche gekennzeichneten elektronischen

Mails nach Ablauf einer verzögernden Zeit weitergeleitet werden.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die Zeitverzögerung in einen vorgegebenen Zeitrahmen fällt, vorzugsweise in die normale Arbeitszeit des Administrators.

- Leerseite -